DMARC SaaS Platform

dmarcian's DMARC SaaS platform receives, processes and classifies mail observed from your domain namespace and makes sense of it for you. The native XML format in which DMARC data is transmitted is not intended for human consumption. Our platform visualizes the data in powerful and meaningful ways so you can quickly identify authentication gaps (SPF/DKIM) and unauthorized use of your domains.

In addition to aggregating DMARC data, our platform provides domain administration teams with the necessary features to adopt DMARC with clarity and confidence. The dmarcian reporting platform sits atop the most accurate source classification engine in the industry and affords users with assurances of the true origin of a particular mail stream.

dmarcian has been processing DMARC data since the inception of the specification in 2012.

Without dmarcian

This – times a whole lot more, depending on the amount of email you send.

With dmarcian

DMARC's XML feedback contains useful information, and **dmarcian** helps you make sense of it.

The Domain Overview contains a summary of the status of all your domains and sources. The geographical location of recent abuse is also shown. View the state of your domains at a glance, and get to work locking down your email domains.

The Detail Viewer allows you to explore your DMARC data in a variety of ways. It shows a timeline of your data along with search parameters such as From and To date selectors, domain and data-provider pickers, and a filter option that can be used to

Getting Started with DMARC

DMARC, (Domain-based Message Authentication Reporting, & Conformance) an open source standard, uses a concept called alignment to tie the result of two other open source standards, SPF (a published list of servers that are authorized to send email on behalf of a domain) and DKIM (a tamper-evident domain seal associated with a piece of email), to the content of an email. If not already deployed, putting a DMARC record into place for your domain will give you feedback that will allow you to troubleshoot your SPF and DKIM configurations if needed.

Adopting DMARC involves creating a DMARC record, publishing it, and using the information that is generated to gain insight and control over the way your domains are handling email. DMARC helps legitimize your email by doing two things:

- Gives feedback about the email itself, including information about SPF and/or DKIM alignment.
- Tells email receivers (like Gmail and Yahoo) how to handle messages that fail to align with those protocols.

dmarcian can assist your organization in every step of the way, from deploying the underlying technologies of DMARC, to making sense of the data that it generates, to gaining full insight and control to the way your email domains are being used.

Assess

The work required to deploy DMARC is directly related to the size and complexity of an organization's email infrastructure. DMARC is a domain-based email control and email domains are a shared resource within most organizations, with use spanning from employees to entire departments, external parties that send email on behalf of the organization, and the organization's own internet-facing applications.

When deploying DMARC, it's best to roll it out across all of an organization's domains instead of focusing on individual domains. When DMARC is deployed at an organization across the entire domain portfolio, the process of deployment itself becomes much easier as there is complete organizational visibility, and managers get new tools to ensure all email is being sent in compliance with the organization's standards.

Publishing a DMARC record

To start generating DMARC data, you must first publish a DMARC record for each domain you wish to monitor. dmarcian's DMARC Record Wizard makes it easy to create a DMARC record.

A DMARC record exists as part of your Domain Name System (DNS) record, which routes traffic on the internet. You can include additional information in the DNS, like your domain's DMARC record—a text entry within the DNS record that tells the world your email domain's policy based on the configured SPF and DKIM protocol.

Here are instructions on how to publish a DMARC record with your DNS host.

Once you've published DMARC records, DMARC data will typically begin to generate within a day or two in the form of reports that give you insight into the way your domains are handling email. These reports are XML-based and can be difficult for humans to read and make sense of, especially when they can number in the thousands. dmarcian's DMARC SaaS Platform specializes in processing these reports and identifying the steps needed so that DMARC can be